BY EXPRESS MAIL NO. EL387308285US
Attorney Docket No. SONY-T0608

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

09/576621 JC936 U.S. PRO
05/31/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年 ５月３１日

出 願 番 号
Application Number: 平成１１年特許願第１５２０６０号

出 願 人
Applicant (s): ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年 ４月１４日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆 彦

出証番号 出証特２０００－３０２５９７７

【書類名】　特許願
【整理番号】　9900443003
【提出日】　平成11年 5月31日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 19/00
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　石黒　隆二
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　岡上　拓巳
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　大石　丈於
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
　【代表者】　出井　伸之
【代理人】
　【識別番号】　100082131
　【弁理士】
　【氏名又は名称】　稲本　義雄
　【電話番号】　03-3369-6479
【手数料の表示】
　【予納台帳番号】　032089
　【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9708842

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理装置および方法、並びに媒体

【特許請求の範囲】

【請求項１】　暗号鍵で暗号化されているデータを蓄積する蓄積手段と、

前記蓄積手段により蓄積されたデータの管理情報を保持する保持手段と、

前記管理情報のうち、所定のタイミングで更新される更新情報を含む演算情報と、前記暗号鍵に基づき所定の演算を行う演算手段と、

前記演算手段の演算結果を記憶する記憶手段と、

前記演算手段の演算結果と、前記記憶手段に記憶されている過去の前記演算結果とを比較し、比較結果に対応して前記蓄積手段に蓄積されている前記データの利用を制御する制御手段と

を備えることを特徴とする情報処理装置。

【請求項２】　前記演算手段は、前記演算情報と前記暗号鍵にハッシュ関数を適用して前記演算を行う

ことを特徴とする請求項１に記載の情報処理装置。

【請求項３】　前記データは音楽データであり、

前記演算情報は、前記音楽データを識別する識別情報を含み、

前記保持手段は、通常、読み出しまたは書き込みを行うことができない領域に前記更新情報を保持する

ことを特徴とする請求項１に記載の情報処理装置。

【請求項４】　暗号鍵で暗号化されているデータを蓄積する蓄積ステップと、

前記蓄積ステップの処理により蓄積されたデータの管理情報を保持する保持ステップと、

前記管理情報のうち、所定のタイミングで更新される更新情報を含む演算情報を、前記暗号鍵に基づき所定の演算を行う演算ステップと、

前記演算ステップの演算結果を記憶する記憶ステップと、

前記演算ステップの演算結果と、前記記憶ステップの処理で記憶された過去の前記演算結果とを比較し、比較結果に対応して前記蓄積ステップの処理で蓄積さ

れた前記データの利用を制御する制御ステップと

を含むことを特徴とする情報処理方法。

【請求項５】　暗号鍵で暗号化されているデータを蓄積する蓄積ステップと、

前記蓄積ステップの処理により蓄積されたデータの管理情報を保持する保持ステップと、

前記管理情報のうち、所定のタイミングで更新される更新情報を含む演算情報を、前記暗号鍵に基づき所定の演算を行う演算ステップと、

前記演算ステップの演算結果を記憶する記憶ステップと、

前記演算ステップの演算結果と、前記記憶ステップの処理で記憶された過去の前記演算結果とを比較し、比較結果に対応して前記蓄積ステップの処理で蓄積された前記データの利用を制御する制御ステップと

を含むことを特徴とするプログラムをコンピュータに実行させる媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報処理装置および方法、並びに媒体に関し、特に、改竄を防止し、不正な複製を抑制することができるようにした、情報処理装置および方法、並びに媒体に関する。

【０００２】

【従来の技術】

最近、デジタル技術の普及にともない、音楽データ、画像データなどの各種のデータがデジタル的に記録媒体に記録または再生されるようになってきた。その結果，複数回コピーしても、画質あるいは音質が劣化しないデータを得ることが可能となってきた。

【０００３】

【発明が解決しようとする課題】

しかしながら、このようにデジタル技術が発達してくると、次のような問題が発生する。

【０００４】

（１）　例えば、コンパクトディスク(CD)からパーソナルコンピュータのハードディスクにデジタル音楽データをコピーする場合、CDからの音楽データが、そのまま、あるいは圧縮符号化されてハードディスクに記録されるので、例えば、インターネットなどのネットワークを介して複製を違法に大量に配布することができてしまう。

【０００５】

（２）　CDからパーソナルコンピュータのハードディスクにデジタル音楽データをコピーする場合、そのコピー回数に制限がないため、複製が大量に配布されてしまう。

【０００６】

（３）　パーソナルコンピュータのハードディスク内のデジタル音楽データを、例えば、メモリスティックウォークマン（商標）などの外部の機器に移す場合、移した後もハードディスク内に元のデジタル音楽データが残るので、複製が大量に配布できてしまう恐れがある。

【０００７】

（４）　上記した（３）の問題を防止するために、デジタル音楽データを外部の機器に移した後に、データの送り元としてのハードディスクのデータを消去するように（いわゆる、音楽データをムーブするように）パーソナルコンピュータのソフトウェアを作成しておけばよいが、例えば，ムーブの前にハードディスクの内容を別の記録媒体へバックアップしておき、ムーブの後に、バックアップしたデータをハードディスクにリストアすれば、結局、ムーブしたはずのデータがハードディスクに残ってしまうことになる。

【０００８】

（５）　パーソナルコンピュータが、ハードディスク内のデジタル音楽データをメモリスティックウォークマンなどの外部の機器に移す場合、外部機器がどのような機器であるかを確認しないため、違法な機器にデジタル音楽データが渡されてしまう恐れがある。

【０００９】

（６）　メモリスティックウォークマンなどの外部の機器から、パーソナルコンピュータにデジタル音楽データを渡す場合、そのパーソナルコンピュータを制御しているソフトウェアがどのようなソフトウェアであるかを確認しないため、違法なソフトウェアに対してデジタル音楽データが渡されてしまう恐れがある。

【００１０】

（７）　CDより再生された音楽データをパーソナルコンピュータで取り扱うとき、複数の曲が同一か否かを判断するために、曲データに含まれるISRC(International Standard Recording Code)を使用することが可能であるが、CDによっては、ISRCデータを含んでいないものがある。この場合、複数の曲が同一であるか否かを判定することができなくなる。

【００１１】

（８）　以上のような各機能は、パーソナルコンピュータ上で、ソフトウェアの制御により実現されるため、そのソフトウェアが改竄されると、システムの作成者が意図しない動作を行わせることができてしまう。

【００１２】

本発明はこのような状況に鑑みてなされたものであり、記録媒体に蓄積されているデータが改竄され、不正に利用されるのを防止することができるようにするものである。

【００１３】

【課題を解決するための手段】

請求項１に記載の情報処理装置は、暗号鍵で暗号化されているデータを蓄積する蓄積手段と、蓄積手段により蓄積されたデータの管理情報を保持する保持手段と、管理情報のうち、所定のタイミングで更新される更新情報を含む演算情報と、暗号鍵に基づき所定の演算を行う演算手段と、演算手段の演算結果を記憶する記憶手段と、演算手段の演算結果と、記憶手段に記憶されている過去の演算結果とを比較し、比較結果に対応して蓄積手段に蓄積されているデータの利用を制御する制御手段とを備えることを特徴とする。

【００１４】

請求項４に記載の情報処理方法は、暗号鍵で暗号化されているデータを蓄積す

る蓄積ステップと、蓄積ステップの処理により蓄積されたデータの管理情報を保持する保持ステップと、管理情報のうち、所定のタイミングで更新される更新情報を含む演算情報を、暗号鍵に基づき所定の演算を行う演算ステップと、演算ステップの演算結果を記憶する記憶ステップと、演算ステップの演算結果と、記憶ステップの処理で記憶された過去の演算結果とを比較し、比較結果に対応して蓄積ステップの処理で蓄積されたデータの利用を制御する制御ステップとを含むことを特徴とする。

【００１５】

請求項５に記載の媒体のプログラムは、暗号鍵で暗号化されているデータを蓄積する蓄積ステップと、蓄積ステップの処理により蓄積されたデータの管理情報を保持する保持ステップと、管理情報のうち、所定のタイミングで更新される更新情報を含む演算情報を、暗号鍵に基づき所定の演算を行う演算ステップと、演算ステップの演算結果を記憶する記憶ステップと、演算ステップの演算結果と、記憶ステップの処理で記憶された過去の演算結果とを比較し、比較結果に対応して蓄積ステップの処理で蓄積されたデータの利用を制御する制御ステップとを含むことを特徴とする。

【００１６】

請求項１に記載の情報処理装置、請求項４に記載の情報処理方法、および請求項５に記載の媒体においては、演算情報と暗号鍵に基づき所定の演算が行われ、その演算結果と、過去の演算結果とが比較され、その比較結果に対応して、蓄積されているデータの利用が制御される。

【００１７】

【発明の実施の形態】

図１は、本発明を適用したネットワークシステムの構成例を表している。パーソナルコンピュータ１は、各種の処理を実行するCPU（Central Processing Unit）１２、各種のプログラムやデータを一時的に記憶するメモリ１３、並びに、各種のプログラムやデータを大量に蓄積するハードディスク１５を備えている。CD-ROM（Read Only Memory）ドライブ１４は、装着されたCD-ROMに記録されているプログラムやデータを読み出す。IEC（International Electrotechnical Commis

sion）６０９５８端子１６ａを有する音声入出力インタフェース１６は、デジタル音声入出力、あるいはアナログ音声入出力のインタフェース処理を実行する。インターネット接続インタフェース１１は、インターネット４との間のインタフェース処理を実行する。インタフェース１７は、アダプタ７またはメモリスティックウォークマン６との間のインタフェース処理、並びに、入力部２およびディスプレイ３に対するインタフェース処理を実行する。

【００１８】

半導体ICとして、一体的に形成され、パーソナルコンピュータ１に装着されるアダプタ７のCPU３２は、インタフェース３１を介してパーソナルコンピュータ１のCPU１２と共働し、各種の処理を実行する。RAM(Random Access Memory)３３は、CPU３２が各種の処理を実行する上において必要なデータやプログラムを記憶する。不揮発性メモリ３４は、パーソナルコンピュータ１の電源がオフされた後も保持する必要があるデータを記憶する。ROM３６には、パーソナルコンピュータ１から、暗号化されているプログラムが転送されてきたとき、それを復号するプログラムが記憶されている。RTC（Real Time Clock）３５は、計時動作を実行し、時刻情報を提供する。

【００１９】

メモリスティックウォークマン６は、不揮発性メモリ（メモリスティック（商標））２３を有し、パーソナルコンピュータ１からインタフェース２１と制御部２２を介して提供されたデジタル音楽データを記憶する。制御部２２は、パーソナルコンピュータ１と不揮発性メモリ２３との間でデータを授受するとき、相互に認証処理を実行する。インタフェース２１は、パーソナルコンピュータ１との間のインタフェース処理、あるいは不揮発性メモリ２３に記憶されている音楽データを読み出し、ヘッドホンなどを介してユーザに提供するためのインタフェース処理を実行する。

【００２０】

パーソナルコンピュータ１は、インターネット４を介してEMD（Electrical Music Distribution）サーバ５と接続されており、EMDサーバ５から音楽データの提供を受けることができる。

【００２１】

次に、メモリスティックウォークマン６の不揮発性メモリ２３に記憶されている音楽データの不正コピーを防止する方法について説明する。

【００２２】

メモリスティックウォークマン６の不揮発性メモリ２３に記憶されている曲ファイルは、図２に示すように、ヘッダ部とデータ部に区分されており、ヘッダ部には、曲識別子（ID）、再生回数、再生期限、曲名、およびアーティスト名などの情報が記憶され、データ部には、暗号化された音楽データなどが記述されている。この例においては、データの改竄を防止するために、曲ファイルのヘッダ部に、MAC（Message Authentication Code）値が記録される。MACは、keyed hashといわれる鍵付き一方向性関数（例えば、SHA、DES等が用いられる）により、式（１）に示すように演算される。

【００２３】

MAC値＝MAC（Ｋｃ,重要情報）　　・・・（１）

ここで、Ｋｃは、データ部に記録されているデータを暗号化しているコンテンツ鍵（暗号鍵）である。また、重要情報は、ヘッダ部に記憶されている情報のうちの所定のもの（例えば、曲識別子、再生回数、および再生期限）である。

【００２４】

図３は、このようなメモリスティックウォークマン６の不揮発性メモリ２３に記録されているデータをパーソナルコンピュータ１により再生する場合の処理を表わしている。ステップＳ１において、パーソナルコンピュータ１のCPU１２、あるいはCPU１２上で動作するアプリケーション（以下の説明では、CPU１２とする）は、メモリスティックウォークマン６の制御部２２と相互認証処理を行い、通信用鍵Ｋｓを共有し、それを利用して、さらに不揮発性メモリ２３のデータ部に記憶されているデータを暗号化している暗号鍵Ｋｃを取得する。

【００２５】

すなわち、CPU１２は、制御部２２と相互認証処理を実行し、通信用鍵Ks_1を共有する。制御部２２は、また、不揮発性メモリ２３と相互認証処理を実行し、

通信用鍵Ｋｓ$_2$を共有する。

【００２６】

相互認証が正しく行われなかったとき、処理は終了されるが、正しく行われたとき、さらに、不揮発性メモリ２３は、内部に記憶している暗号鍵Ｋｃ（保存用鍵で暗号化されている）を、やはり内部に記憶している保存用鍵で復号し、通信用鍵Ｋｓ$_2$で暗号化して、制御部２２に転送する。制御部２２は、転送を受けた暗号鍵Ｋｃを通信用鍵Ｋｓ$_2$で復号する。

【００２７】

また、このとき、不揮発性メモリ２３は、曲ファイルのヘッダ部に記憶されている重要情報と前回のMAC値を読み出し、通信用鍵Ｋｓ$_2$で暗号化して制御部２２に転送する。制御部２２は、これを受信すると、通信用鍵Ｋｓ$_2$で復号する。

【００２８】

制御部２２は、暗号鍵Ｋｃ、重要情報、および前回のMAC値を、通信用鍵Ｋｓ$_1$で暗号化し、CPU１２に転送する。CPU１２は、これを通信用鍵Ｋｓ$_1$で復号する。

【００２９】

このように、不揮発性メモリ２３と制御部２２の間、または、制御部２２とCPU１２（アプリケーション）との間は、それぞれ通信用鍵Ｋｓ$_2$、または通信用鍵Ｋｓ$_1$で暗号化して、データが授受されるが、以下の説明においては、この暗号化処理の説明は、特に強調する必要がある場合を除き、省略する。

【００３０】

ステップＳ２において、CPU１２は、ステップＳ１で取得した暗号鍵Ｋｃと、曲ファイルのヘッダ部の重要情報とから、上記した式（１）に従って、MAC値を演算し、その値をＲに設定する。ステップＳ３において、CPU１２は、ステップＳ２で演算された値Ｒと、前回演算され、曲ファイルのヘッダ部に保存されていたMAC値とを比較する。両者が一致しない場合、CPU１２は、ステップＳ４に進み、例えば、「曲ファイルが改竄された恐れがあります」のようなメッセージを、ディスプレイ３に表示させた後、処理を終了させる。この場合においては、メモリスティックウォークマン６の不揮発性メモリ２３に記録されている音楽データ

は、改竄されたものであり、再生が実行されない。

【００３１】

値Ｒと曲ファイルのヘッダ部に保存しておいたMAC値が一致すると判定された場合、ステップＳ５に進み、CPU１２は、制御部２２を介して、不揮発性メモリ２３から、暗号化されている音楽データの転送を受け、それを暗号鍵Ｋｃで復号し、音声入出力インタフェース１６を介して出力（再生）する。

【００３２】

ステップＳ６において、CPU１２は、制御部２２を制御し、不揮発性メモリ２３の曲ファイルのヘッダ部の重要情報の中の再生回数の値を１だけインクリメントさせる。さらに、CPU１２は、ステップＳ７において、制御部２２を制御し、新たな重要情報（その再生回数の値が１だけインクリメントされている）を用いて、式（１）に従って、MAC値を演算させ、そのMAC値で、不揮発性メモリ２３の曲ファイルのヘッダ部に保存されているMAC値を更新させる。MAC値は、暗号鍵Ｋｃがないと演算できないため、認証を受けた機器あるいはアプリケーションだけが、演算できることになる。

【００３３】

しかしながら、図３の方法は、図４に示した方法による不正を防止することができない。すなわち、まず、最初に不揮発性メモリ２３－１の曲ファイル（そのMAC値として、MAC１が記録されているものとする）がハードディスク１５にバックアップされたとすると、これがハードディスク１５に、曲ファイル１（MAC１）として記憶される。このとき、不揮発性メモリ２３－１には、オリジナルの曲ファイル（MAC１）が残る。

【００３４】

次に、不揮発性メモリ２３－１の曲ファイル（MAC１）がハードディスク１５に移動されると、これが、ハードディスク１５に、曲ファイル２（MAC１）として記憶される。このとき、不揮発性メモリ２３－１の曲ファイル（MAC１）は削除され、ハードディスク１５には、曲ファイル１（MAC１）と曲ファイル２（MAC１）の２つの曲ファイルが記憶される。

【００３５】

さらに、ハードディスク１５の曲ファイル１（MAC１）が不揮発性メモリ２３－１にリストアされると、ハードディスク１５には曲ファイル２（MAC１）が残る。ハードディスク１５の曲ファイル２（MAC１）が他の不揮発性メモリ２３－２に移動されると、結果的に、同一の曲ファイル（MAC１）が２つの不揮発性メモリ２３－１，２３－２に記憶されたことになる。従って、不揮発性メモリ２３－２に記憶された曲ファイル２（MAC１）を、不揮発性メモリ２３－１に記憶された曲ファイル１（MAC１）と同様に再生することができる。

【００３６】

このような不正を防止するために、例えば、MAC値を、次式（２）で示すようにして求めることができる。式（２）において、変数seq#は、コピーや移動が行われる毎に更新（例えばインクリメント）される変数であり、不揮発性メモリ２３の、通常のアプリケーションによるアクセスが禁止されている（アダプタ７または認証を受けたアプリケーションのみがアクセス可能な）media defect list（メディア　ディフェクト　リスト）の０番目のblockに記憶される。また、||は連結（または結合）を意味し、A||Bは、データA（ａビット）の最下位ビット（LSB（Least Significant Bit））側にデータＢ（ｂビット）を単純に結合して、a＋ｂビットにしたデータを意味する。

【００３７】

MAC値＝MAC（Ｋｃ，seq# || 重要情報）　　・・・（２）

media defect list は、図５（Ａ）に示すように、defect（bad） block（欠陥を有するブロック）と、その交代ブロックを登録しておくリストで、基本的に、ここにdefect blockとして登録されると、そのblockに対する読み出しおよび書き込みは禁止され、その代わりに、交代ブロックに対して読み出しおよび書き込みが行われる。ただし、０番目のdefect blockには、欠陥を有しないblockが登録されており、制御部２２は、特別なコマンドを受信したときにだけ、そこに対する読み出しおよび書き込みを実行するようになされている。変数seq#は、図５（Ｂ）に示すように、この０番目のdefect blockに記憶される。

【００３８】

この特別な指令（コマンド）を出すことができるのは、アダプタ７と認証を受

けたアプリケーションだけとされる。従って、０番目のdefect blockにアクセスすることができるのは、アダプタ７と認証を受けたアプリケーションだけとなる。

【００３９】

変数seq#は、それぞれの曲（トラック）に対して、一対一に割り振られているため、MAC値の再演算は、その各曲（トラック）毎に行われる。

【００４０】

なお、変数seq#を記憶する領域は、media defect listの０番目のdefect blockに限られるものではなく、一般的に、読み出しおよび書き込みが禁止される領域であれば、それらを利用しても良い。

【００４１】

図６は、このような不揮発性メモリ２３に記録されている曲ファイルをハードディスク１５に移動する場合の処理を表わしている。

【００４２】

ステップＳ２１において、制御部２２は、メモリスティック（不揮発性メモリ２３）と認証し、暗号鍵Ｋｃを取得する。ステップＳ２２において、パーソナルコンピュータ１のCPU１２、あるいはパーソナルコンピュータ１に搭載されているアプリケーション（以下の説明では、アプリケーションとする）は、メモリスティックウォークマン６（制御部２２）と相互認証処理を行い、通信用鍵Ｋｓを共有する。この処理は、上述した図３のステップＳ１の処理と同様の処理である（但し、ステップＳ１では、このとき共有する通信用鍵をKs_1としている）。

【００４３】

ステップＳ２３において、アプリケーション（認証されている）は、制御部２２に特別なコマンドを出力し、不揮発性メモリ２３のmedia defect listの０番目のdefect blockに記憶されている変数seq#を、所定の値に更新させる。

【００４４】

ステップＳ２４において、制御部２２は、ステップＳ２１で不揮発性メモリ２３から取得した暗号鍵Ｋｃを、ステップＳ２２との間で取得した通信用鍵Ｋｓで暗号化し、アプリケーションへ転送する。ステップＳ２５において、制御部２２

は、不揮発性メモリ２３に記憶されている曲ファイルのデータ部の、暗号化されている音楽データの転送を受け、通信用鍵Ｋｓで暗号化して、アプリケーションへ転送し、ハードディスク１５にコピーさせる。ステップＳ２６において、アプリケーションは、メモリスティックウォークマン６から転送されてきた暗号鍵Ｋｃを通信用鍵Ｋｓで復号し、自分自身の保存用鍵で暗号化し、ハードディスク１５に記憶する。

【００４５】

ステップＳ２７において、アプリケーションは、制御部２２に対して、音楽データがコピーされたことを通知する。このとき制御部２２は、ステップＳ２８において、不揮発性メモリ２３に記憶されている曲ファイル（ステップＳ２５で、アプリケーションに転送した曲ファイル）を削除する。

【００４６】

移動処理をこのように行うようにすると、図４を参照して説明した不正コピーを防止することができる。いま、例えば、図７に示すように、不揮発性メモリ２３－１に曲Ａが記録されているものとする。この場合、曲Ａの重要情報に対応するMAC値としてのMAC１が曲Ａのヘッダ部に保存され、変数seq１が、media defect listの０番目のdefect blockに、曲Ａに対応して記憶されている（以下、この場合の状態を、“Ａ（MAC１），seq１”のように記述する）。この状態において、記録データ（曲ファイル）をハードディスク１５にバックアップしたとする。このとき、ハードディスク１５には曲Ａ（MAC１）が記憶されているが、不揮発性メモリ２３の変数seq１とMAC１は更新されていないので、不揮発性メモリ２３－１には、曲Ａ（MAC１），seq１が残る。

【００４７】

次に、不揮発性メモリ２３－１の曲Ａ（MAC１），seq１をハードディスク１５に移動させた場合、その時点において、不揮発性メモリ２３－１の変数seq１は、変数seq２に更新される（ステップＳ２３）が、MAC１は更新されていないので、ハードディスク１５には、曲Ａ（MAC１）が、新たに記録される。制御部２２は、アプリケーションからの通知（曲Ａが移動された旨の通知）を受け、不揮発性メモリ２３－１に記録されている曲Ａを削除させる。

【００４８】

その後、ハードディスク１５にバックアップされた曲Ａ（MAC１）を不揮発性メモリ２３－１にリストアすると、不揮発性メモリ２３－１には、曲Ａ（MAC１），seq２が保存される。さらに、ハードディスク１５に移動された曲Ａ（MAC１）を他の不揮発性メモリ２３－２に移動させると、変数seq２が、さらに変数seq３に更新され、記録される曲は、曲Ａ（MAC１），seq３となる。

【００４９】

この不揮発性メモリ２３－１または２３－２が、図３のフローチャートに沿って再生されると、ステップＳ２の処理でMAC値の演算には、変数seq２（またはseq３）が用いられることになり、変数seq１を用いて演算され、曲ファイルのヘッダ部に記憶されているMAC１とは異なる値となる。その結果、ステップＳ３で判定がNOになり、この曲は不正にコピーされたとして、再生されることはない。

【００５０】

以上においては、記録媒体として、メモリスティックウォークマン６の不揮発性メモリ（メモリスティック）２３を用いる場合を例として説明したが、本発明は、その他の記録媒体にデータを移転またはコピーする場合にも応用することが可能である。

【００５１】

また、データは、音楽データ以外に、画像データ、その他のデータとすることもできる。

【００５２】

上述した一連の処理は、ハードウエアにより実行させることもできるが、ソフトウエアにより実行させることもできる。一連の処理をソフトウエアにより実行させる場合には、そのソフトウエアを構成するプログラムが、専用のハードウエアとしてのメモリスティックウォークマン６に組み込まれているコンピュータ（制御部２２に対応する）、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどにインストールされる。

【００５３】

次に、図８を参照して、上述した一連の処理を実行するプログラムをコンピュータにインストールし、コンピュータによって実行可能な状態とするために用いられる媒体について、そのコンピュータが汎用のパーソナルコンピュータである場合を例として説明する。

【００５４】

プログラムは、図８（Ａ）に示すように、パーソナルコンピュータ５１に内蔵されている記録媒体としてのハードディスク５２（図１のパーソナルコンピュータ１に内蔵されているハードディスク１５に対応する）や半導体メモリ５３に予めインストールした状態でユーザに提供することができる。

【００５５】

あるいはまた、プログラムは、図８（Ｂ）に示すように、フロッピーディスク６１、CD-ROM６２、MO（Magneto-Optical）ディスク６３、DVD（Digital Versatile Disk）６４、磁気ディスク６５、または半導体メモリ６６などの記録媒体に、一時的あるいは永続的に格納し、パッケージソフトウエアとして提供することができる。

【００５６】

さらに、プログラムは、図８（Ｃ）に示すように、ダウンロードサイト７１から、デジタル衛星放送用の人工衛星７２を介して、パーソナルコンピュータ５１に無線で転送したり、ローカルエリアネットワーク、インターネットといったネットワーク８１を介して、パーソナルコンピュータ５１に有線で転送し、パーソナルコンピュータ５１おいて、内蔵するハードディスク５２などに格納させることができる。

【００５７】

本明細書における媒体とは、これら全ての媒体を含む広義の概念を意味するものである。

【００５８】

パーソナルコンピュータ５１は、例えば、図９に示すように、CPU９２を内蔵している。CPU９２にはバス９１を介して入出力インタフェース９５が接続されており、CPU９２は、入出力インタフェース９５を介して、ユーザから、キーボ

ード、マウスなどよりなる入力部９７から指令が入力されると、それに対応して、図８（Ａ）の半導体メモリ５３に対応するROM９３に格納されているプログラムを実行する。あるいはまた、CPU９２は、ハードディスク５２に予め格納されているプログラム、人工衛星７２もしくはネットワーク８１から転送され、通信部９８により受信され、さらにハードディスク５２にインストールされたプログラム、またはドライブ９９に装着されたフロッピーディスク６１、CD-ROM６２、MOディスク６３、DVD６４、もしくは磁気ディスク６５から読み出され、ハードディスク５２にインストールされたプログラムを、RAM９４にロードして実行する。さらに、CPU９２は、その処理結果を、例えば、入出力インタフェース９５を介して、LCD（Liquid Crystal Display）などよりなる表示部９６に必要に応じて出力する。

【００５９】

なお、本明細書において、媒体により提供されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【００６０】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【００６１】

【発明の効果】

請求項１に記載の情報処理装置、請求項４に記載の情報処理方法、および請求項５に記載の媒体によれば、演算情報と暗号鍵に基づき所定の演算を行い、その演算結果と、過去の演算結果とを比較し、その比較結果に対応して、蓄積されているデータの利用を制御するようにしたので、改竄が行われたとしても、それを検出することができ、蓄積されているデータの不正な複製を防止することが可能となる。

【図面の簡単な説明】

【図１】

本発明を適用したシステムの構成例を示すブロック図である。

【図２】

曲ファイルを説明する図である。

【図３】

図１のメモリスティックウォークマン６からパーソナルコンピュータ１にデータを出力する場合の処理を説明するフローチャートである。

【図４】

図３の処理に関する不揮発性メモリ２３の動作を説明する図である。

【図５】

media defect listを説明する図である。

【図６】

図１のメモリスティックウォークマン６からハードディスク１５へデータを移動する場合の処理を説明するフローチャートである。

【図７】

図６の処理に関する不揮発性メモリ２３の動作を説明する図である。

【図８】

媒体を説明する図である。

【図９】

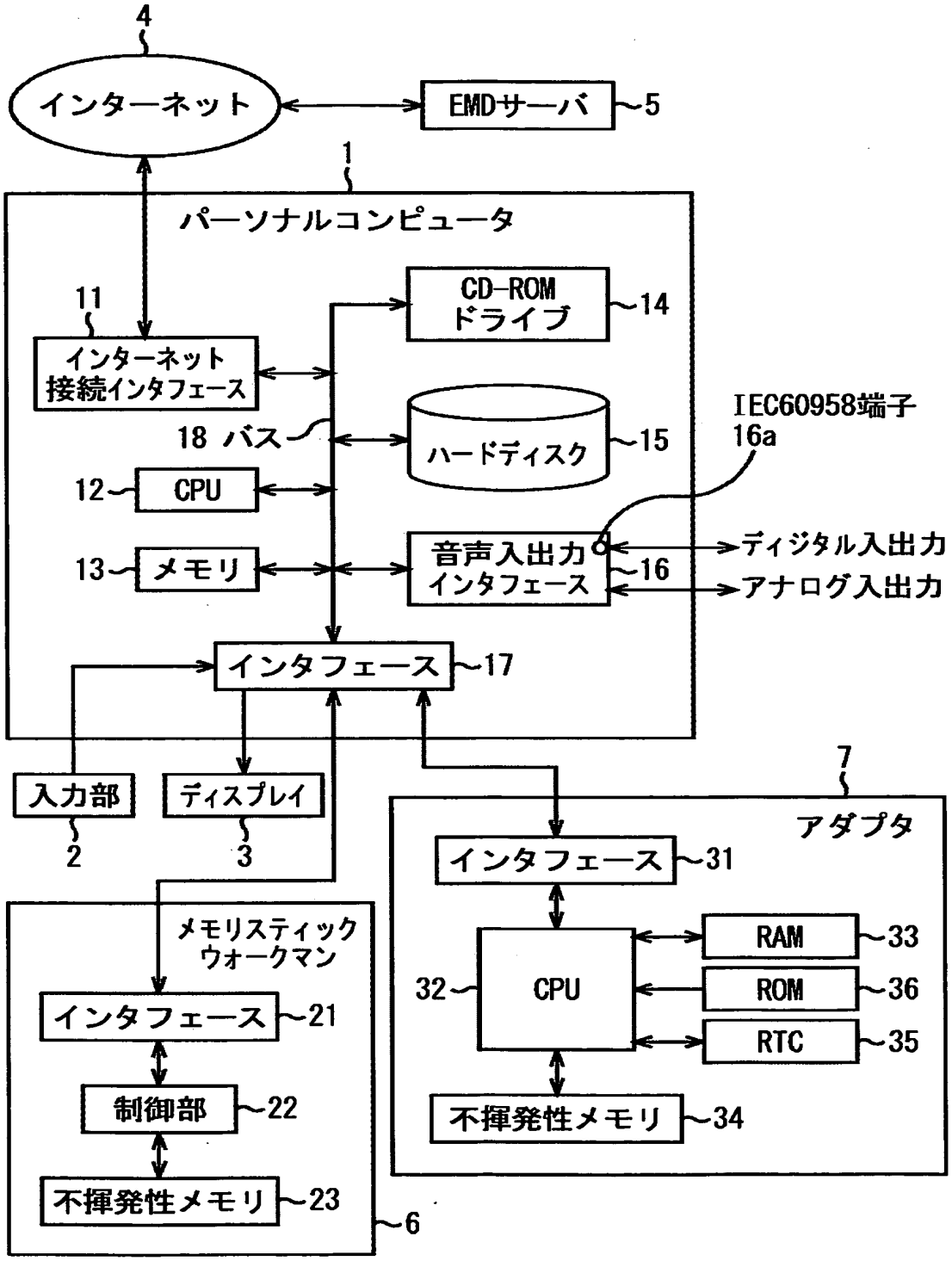
図８のパーソナルコンピュータ５１の構成を示すブロック図である。

【符号の説明】

１　パーソナルコンピュータ，　２　入力部，　３　ディスプレイ，　４　インターネット，　５　EMDサーバ，　６　メモリスティックウォークマン，　７　アダプタ，　１２　CPU，　１３　メモリ，　１４　CD-ROMドライブ，　１５　ハードディスク，　１６　音声入出力インタフェース，　１６ａ　IEC６０９５８端子，　２２　制御部，　２３－１，２３－２　不揮発性メモリ，　３２　CPU

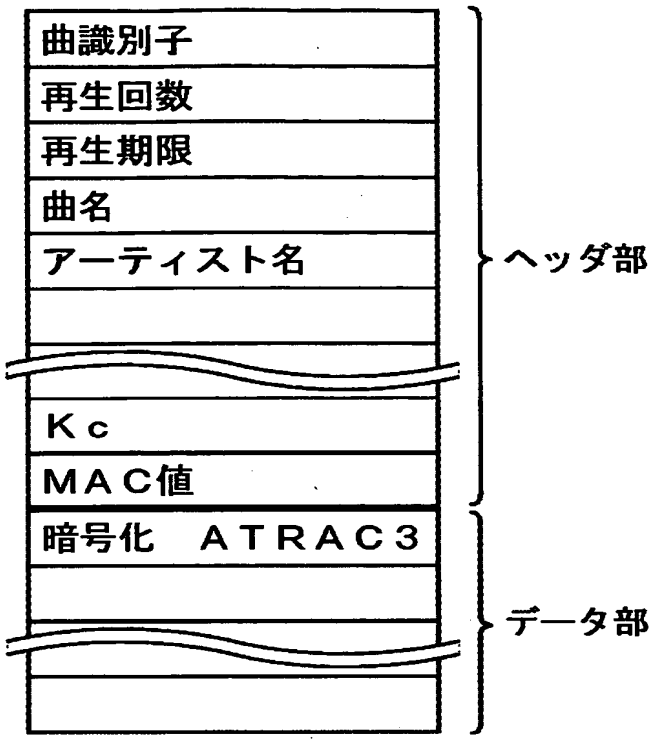
【書類名】図面

【図１】


4
インターネット
EMDサーバ
5
1
パーソナルコンピュータ
11
インターネット
接続インタフェース
CD-ROM
ドライブ
14
18 バス
ハードディスク
15
IEC60958端子
16a
12
CPU
13
メモリ
音声入出力
インタフェース
16
ディジタル入出力
アナログ入出力
インタフェース
17
入力部
2
ディスプレイ
3
7
アダプタ
インタフェース
31
32
CPU
RAM
33
ROM
36
RTC
35
不揮発性メモリ
34
メモリスティック
ウォークマン
インタフェース
21
制御部
22
不揮発性メモリ
23
6

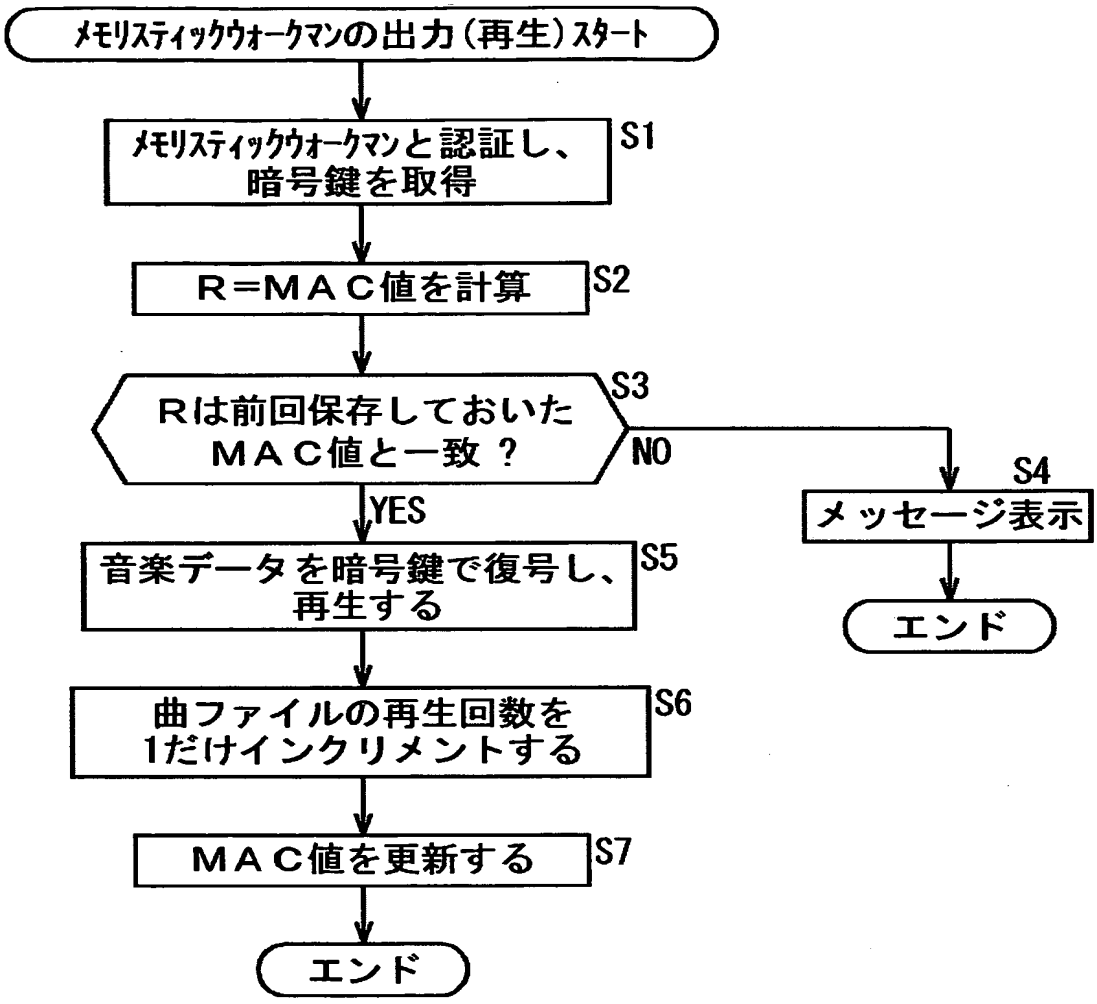
【図２】

曲ファイル

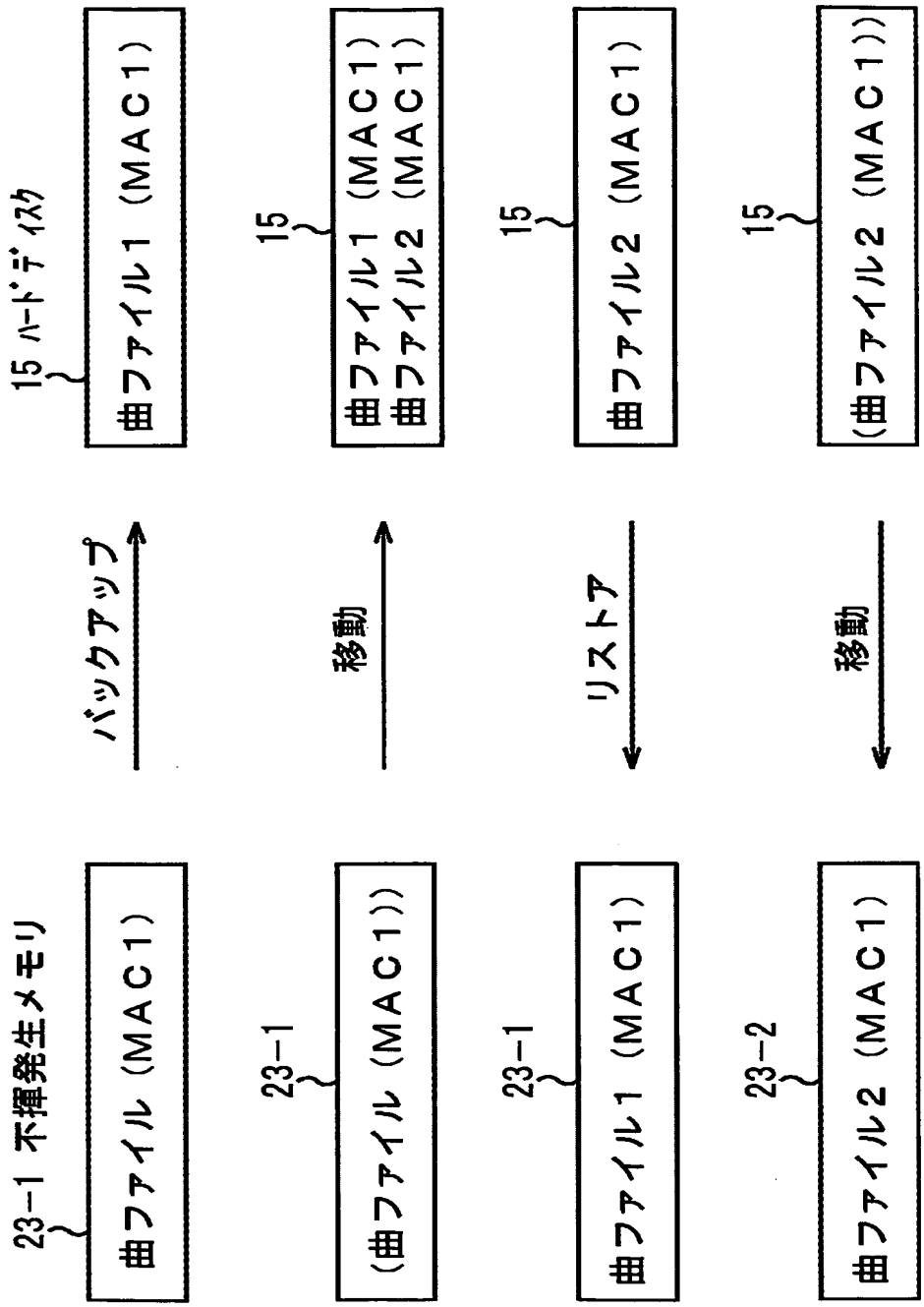


出証特２０００－３０２５９７７

【図３】


メモリスティックウォークマンの出力（再生）スタート
メモリスティックウォークマンと認証し、暗号鍵を取得
S1
R＝ＭＡＣ値を計算
S2
Rは前回保存しておいたＭＡＣ値と一致？
S3
NO
YES
S4
メッセージ表示
エンド
音楽データを暗号鍵で復号し、再生する
S5
曲ファイルの再生回数を1だけインクリメントする
S6
ＭＡＣ値を更新する
S7
エンド

【図４】


15 ハードディスク
曲ファイル１（ＭＡＣ１）
15
曲ファイル１（ＭＡＣ１）
曲ファイル２（ＭＡＣ１）
15
曲ファイル２（ＭＡＣ１）
15
（曲ファイル２（ＭＡＣ１））
バックアップ
移動
リストア
移動
23－1 不揮発生メモリ
曲ファイル（ＭＡＣ１）
23－1
（曲ファイル（ＭＡＣ１））
23－1
曲ファイル１（ＭＡＣ１）
23－2
曲ファイル２（ＭＡＣ１）

【図５】

（Ａ）

Media defect list

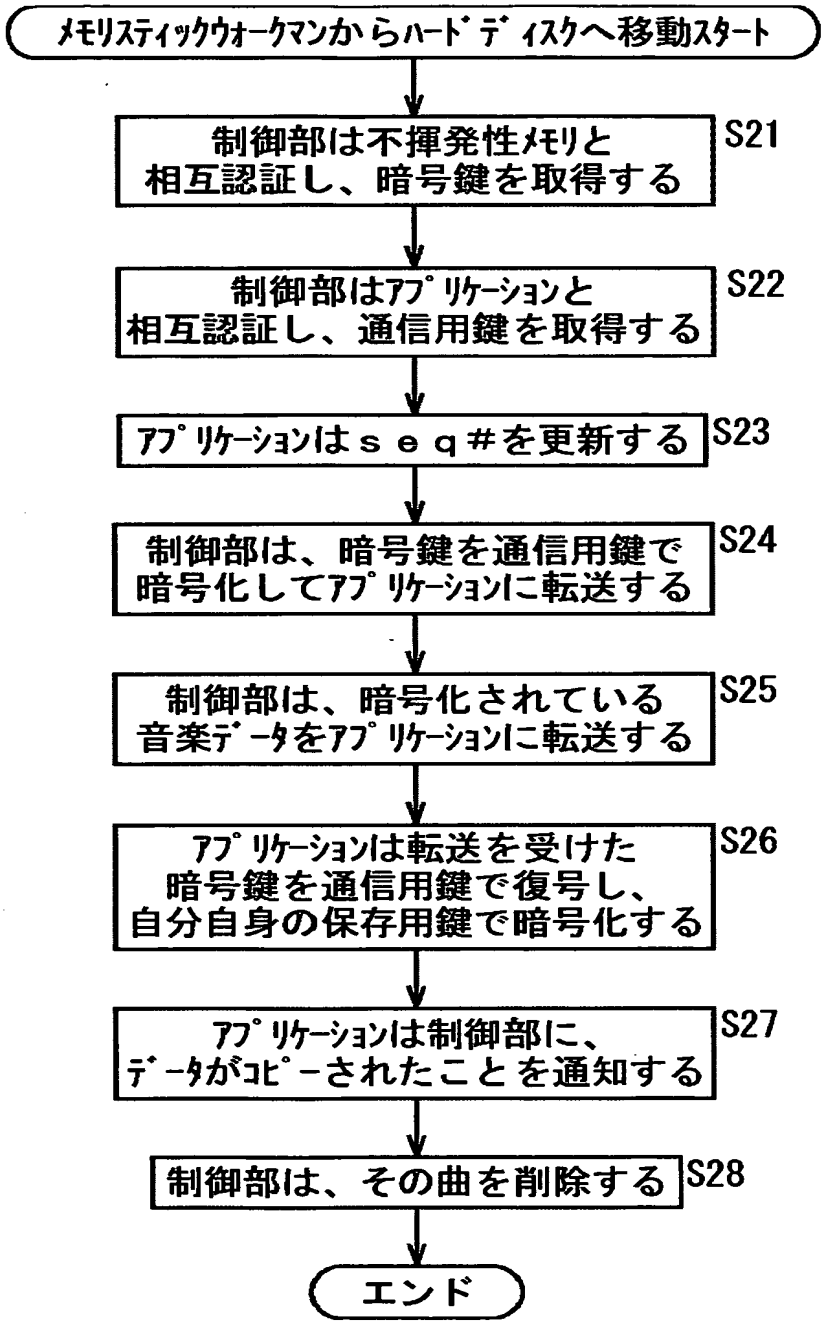
	defect (bad) block	交代ブロック
0		
1		
2		
3		
4		
5		

（Ｂ）

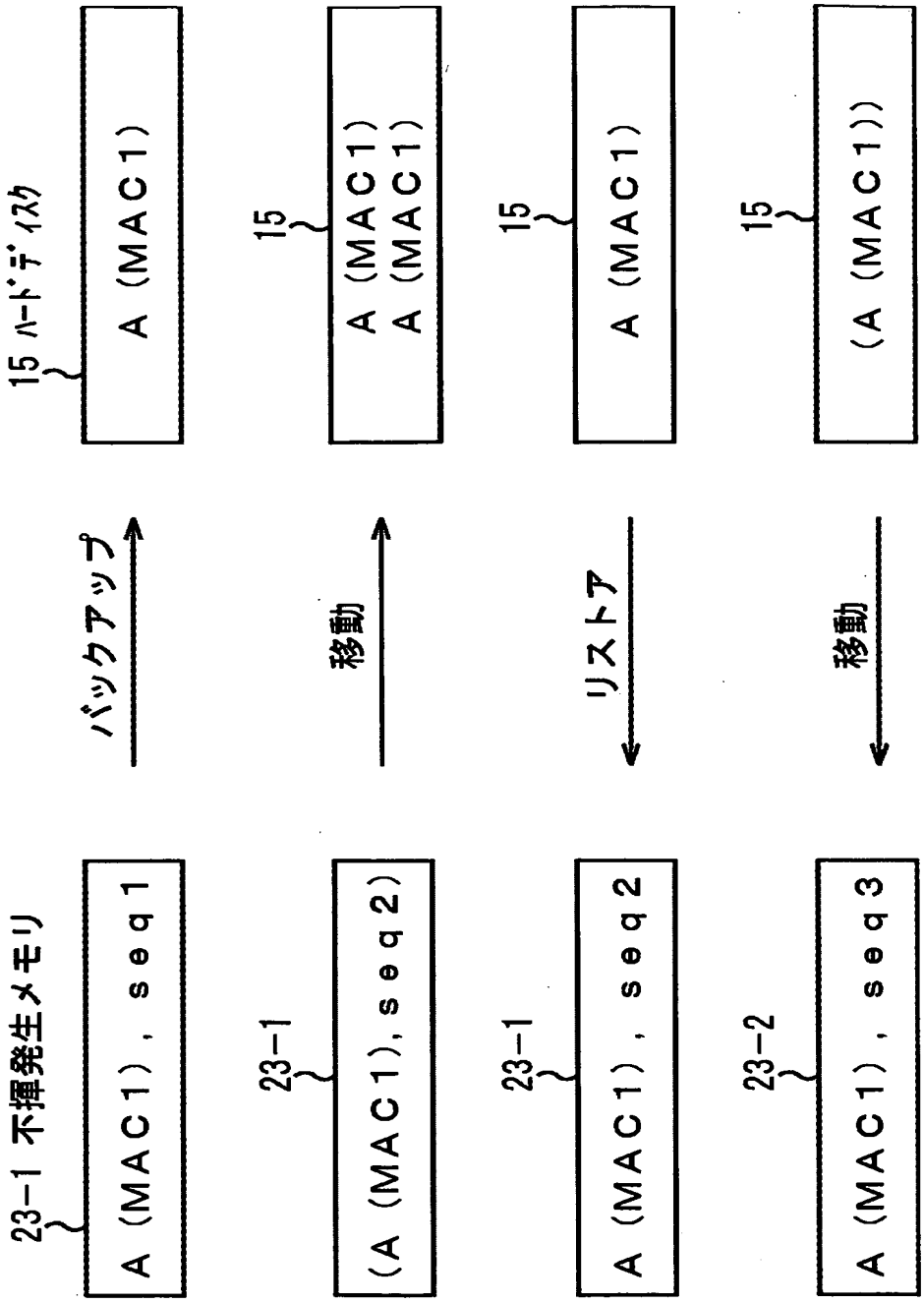
0番目defect block

ｓｅｑ１
ｓｅｑ２
ｓｅｑ３
ｓｅｑ４

【図６】

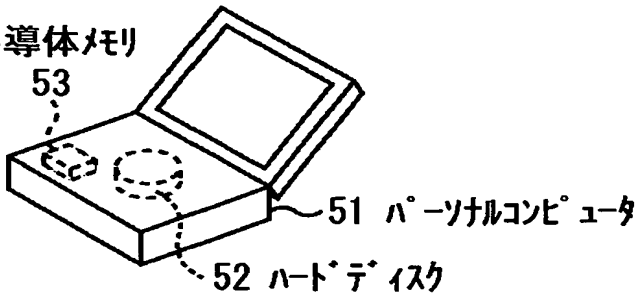

メモリスティックウォークマンからハードディスクへ移動スタート
制御部は不揮発性メモリと相互認証し、暗号鍵を取得する
S21
制御部はアプリケーションと相互認証し、通信用鍵を取得する
S22
アプリケーションはｓｅｑ＃を更新する
S23
制御部は、暗号鍵を通信用鍵で暗号化してアプリケーションに転送する
S24
制御部は、暗号化されている音楽データをアプリケーションに転送する
S25
アプリケーションは転送を受けた暗号鍵を通信用鍵で復号し、自分自身の保存用鍵で暗号化する
S26
アプリケーションは制御部に、データがコピーされたことを通知する
S27
制御部は、その曲を削除する
S28
エンド

【図７】

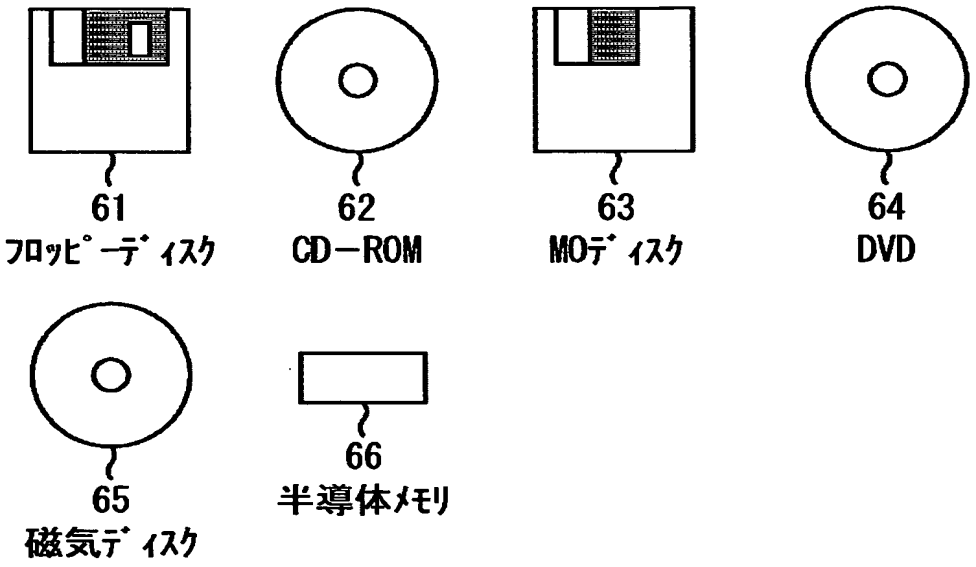

15 ハードディスク
A（MAC1）
バックアップ
23-1 不揮発生メモリ
A（MAC1），seq1
15
A（MAC1）
A（MAC1）
移動
23-1
（A（MAC1），seq2）
15
A（MAC1）
リストア
23-1
A（MAC1），seq2
15
（A（MAC1））
移動
23-2
A（MAC1），seq3

【図８】

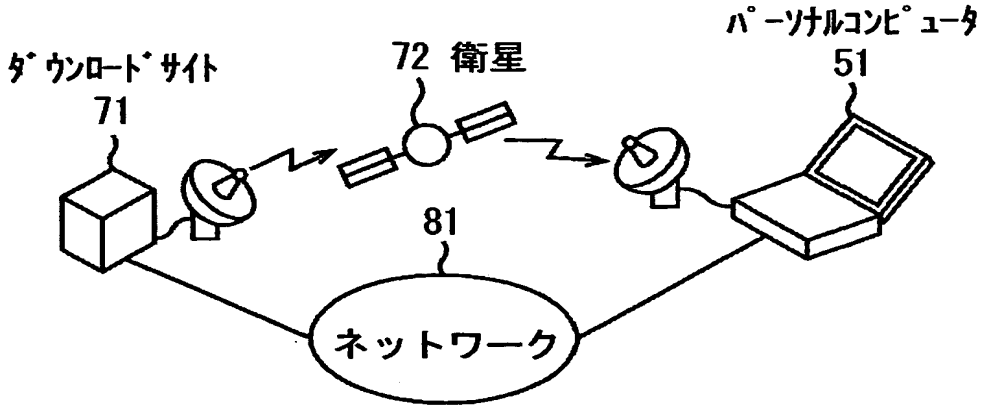
（Ａ）


半導体メモリ
53
51 パーソナルコンピュータ
52 ハードディスク

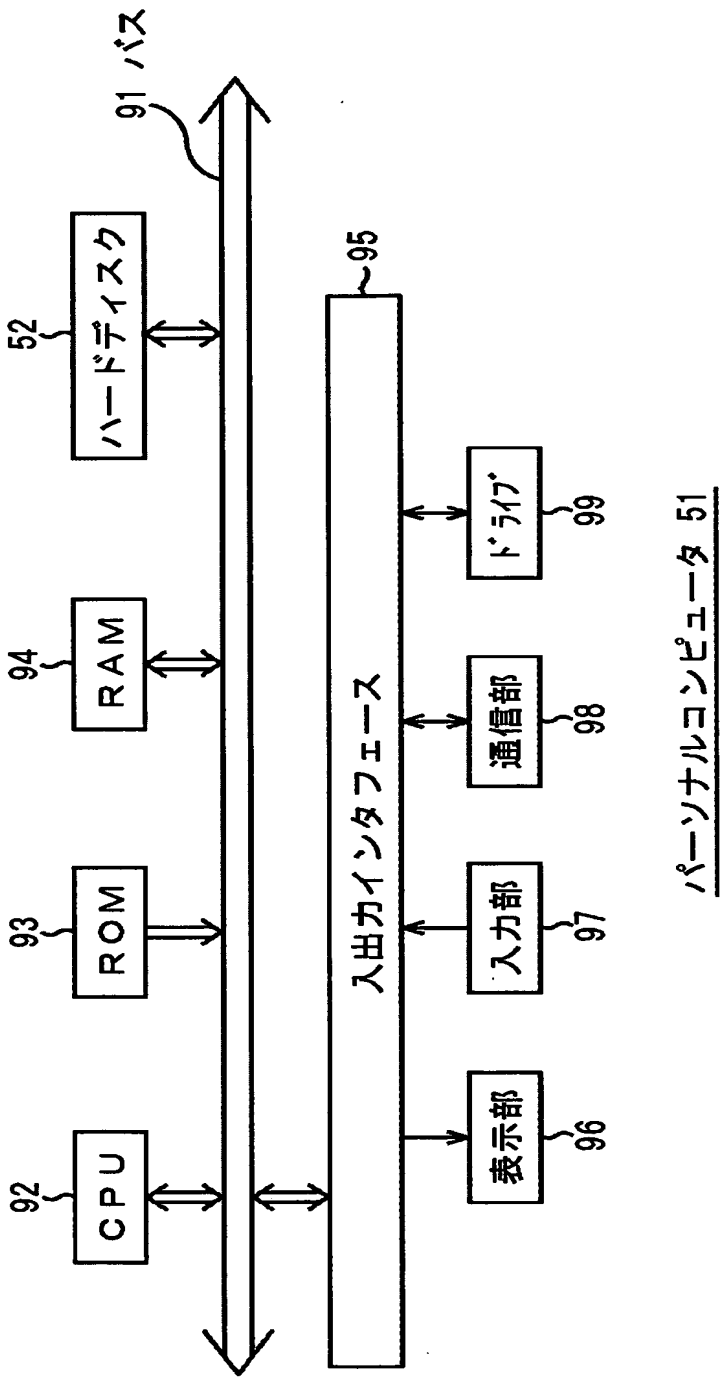
（Ｂ）


61
フロッピーディスク
62
CD－ROM
63
MOディスク
64
DVD
65
磁気ディスク
66
半導体メモリ

（Ｃ）


ダウンロードサイト
71
72 衛星
パーソナルコンピュータ
51
81
ネットワーク

【図９】


91 バス
52 ハードディスク
95
94 RAM
93 ROM
92 CPU
入出力インタフェース
ドライブ 99
通信部 98
入力部 97
表示部 96
パーソナルコンピュータ 51

【書類名】　　要約書

【要約】

【課題】　蓄積されているデータが改竄され、不正に利用されるのを防止する。

【解決手段】　不揮発性メモリ２３－１からハードディスク１５に曲を移動するとき、アプリケーションは、不揮発性メモリ２３－１のmedia defect listの０番目のdefect blockに記憶されている変数seq１を、新たな値seq２に更新する。アプリケーションは、不揮発性メモリ２３－１のデータ部に記憶されている音楽データを暗号化している暗号鍵と、変数seq#を含む重要情報とからMAC値（ハッシュ値）を演算し、その値と、ヘッダ部に記憶されているMAC値とを比較し、両者が一致しなければ、音楽データの再生を禁止する。

【選択図】　　図７

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社